

Reuse of safety certification artefacts across standards and domains: A systematic approach

Alejandra Ruiz, Garazi Juez, Huáscar Espinoza
ICT Division, TECNALIA
Derio, Spain
{name.surname}@tecnalia.com

Jose Luis de la Vara
Computer Science Department, Carlos III University of Madrid,
Leganés, Madrid, Spain
jvara@inf.uc3m.es

Xabier Larrucea
Escuela Universitaria de Ingeniería, Universidad del País Vasco,
Vitoria, Spain
xabier.larrucea@ehu.eus
ICT Division, TECNALIA
Derio, Spain
Xabier.larrucea@tecnalia.com

Abstract—Reuse of systems and subsystem is a common practice in safety-critical systems engineering. Reuse can improve system development and assurance, and there are recommendations on reuse for some domains. Cross-domain reuse, in which a previously certified product typically needs to be assessed against different safety standards, has however received little attention. No guidance exists for this reuse scenario despite its relevance in industry, thus practitioners need new means to tackle it. This paper aims to fill this gap by presenting a systematic approach for reuse of safety certification artefacts across standards and domains. The approach is based on the analysis of the similarities and on the specification of maps between standards. These maps are used to determine the safety certification artefacts that can be reused from one domain to another and reuse consequences. The approach has been validated with practitioners in a case study on the reuse of an execution platform from railway to avionics. The results show that the approach can be effectively applied and that it can reduce the cost of safety certification across standards and domains. Therefore, the approach is a promising way of making cross-domain reuse more cost-effective in industry.

Keywords: safety-critical system, safety certification, safety assurance, reuse, safety standard, cross-domain.

1 INTRODUCTION

Safety-critical systems are those whose failure could end up in loss or injuries to people or the environment. These systems are usually required to go through certification processes, or safety assurance processes in general, according to some safety (or safety-related) standard [1]. The goal of certification is to provide the different stakeholders, including the society, the assurance that a system does not introduce unacceptable risks of catastrophic consequences [2]. Prescriptive standards such as DO-178C in avionics [3] or the general IEC 61508 standard [4] define processes and specific evidence to show compliance. Other standards follow a goal-based strategy where the achievement of compliance and of a system's safety objectives is documented in an assurance case. This case roughly consists of arguments that justify compliance and system safety, are supported by evidence, and are evaluated by a certification body. An example of this second approach is the Def 00-56 military standard [5]. It is also common that specific domains have their own applicable standards, such as EN 50128 for railway [6] and ISO 26262 for automotive [7].

Certification processes are laborious and expensive, and tend to increase the effort and cost to develop safety-critical systems. For example, Boeing's 787 Dreamliner aircraft needed a certification assessment process that lasted eight years in order to obtain the airworthiness certificate [8]. During that process, the Federal Aviation Agency reported about 200,000 hours of technical work on type certificate, which were exceeded by the hours required by technicians from the company. Boeing needed to present more than 4,000 documents to show evidence of compliance, including plans, flight test reports and safety analyses. The total effort and cost for system certification are higher if all the different stakeholders of the supply chain (e.g. component suppliers) are taken into account e.g. for component qualification.

Safety-critical systems are typically not built up from scratch as a massive and unique element, but as a composition of systems and subsystems working in collaboration. This decomposition into subsystems introduces a good chance for reuse, where the effort needed for compliance can be assumed by the different systems in which a subsystem or component is used or reused. We are considering system as in avionics, i.e. as a self-contained part, combination of parts, subassemblies, or units that performs a distinct function of a system [3]. In order to reduce the time needed to put a new system into the market, reuse of e.g. software improves productivity and reliability of development projects and lowers their overall cost. These benefits could increase up to 50% with a high level of reuse [9]. There is guidance on how to reuse components and subsystems in domains such as automotive [7] and avionics [10].

Not only the certification investment can benefit from reuse but also other advantages have been recognised [11]:

- Dependability property improvement. Systems and components are thoroughly verified and proved each time they are reused. The historical data of their performance and of reactions to vulnerabilities also increases, providing the system or component developer with exact data to improve dependability.
- Process risk reduction. When following a reuse strategy, the risk is shared by each of the times that the reuse has been performed. Even more, reuse supports the application of process best practices, mitigating the process risk associated.
- Effective use of specialists. The knowledge is encapsulated in the different components and associated artefacts that are reused, liberating this way a specialist from monotonous work. Specialists can focus on challenging areas where their knowledge is especially needed.
- Accelerated development. The time to market of a product is reduced by reusing previously developed projects or part of projects.

Difficulty in deciding if a component can be reused and provision of safety evidence for systems that reuse existing systems and components have been acknowledged as challenges both in the literature [12] and by practitioners [13,14]. It is also considered that industry needs more systematic approaches for safety certification artefact (aka evidence) reuse [15]. A major issue arises when aiming to reuse, in a given domain, a system that has been previously certified and deployed in another domain. This is mainly due to the differences between the applicable safety standards and thus between the certification requirements.

Although effective cross-domain reuse is gaining attention in industry [16] and seems to be a re-certification scenario in which many practitioners dealing with safety evidence change impact analysis have been involved [14], there are no recommendations or guidance offered by certification authorities in order to facilitate product reuse across different domains. Originally the suppliers used to work in only one domain but now the trend has changed. The providers are more and more interested in widening their market and in providing their products across different domains in an efficient way, including the certification. Cross-domain certification is even more challenging when auditors and assessors aim to identify the required evidence for certifying a system against the target certification scheme, based on the evidence provided for the source scheme. Without a valid analysis and understanding of safety evidence reuse consequences, a system will need to go through the entire certification process of the target domain. This will require a considerable amount of time and resources, reducing the benefits of product reuse. These issues generally apply to re-certification of a system against a different safety standard. This can occur both in cross-domain reuse and in a single domain, where standards and certification schemes might e.g. vary among countries.

This paper aims to contribute to addressing the above issues by proposing a novel approach that assists on the systematic reuse of compliance justifications and safety certification artefacts across standards and domains (hereafter referred to as reuse approach). The approach has been developed in the scope of OPENCROSS (<http://www.opencross-project.eu>), which is a European industry-academia project on evolutionary certification of safety-critical systems for automotive, avionics, and railway. OPENCROSS industry stakeholders have provided input for designing the reuse approach and have contributed to its validation.

The reuse approach is based on the specification of how similar two safety standards are by mapping them. A pair of safety standards can have commonalities and differences, thus their safety criteria can be fully or partially similar or no map might exist. The resulting maps can be later exploited to determine the extent to which compliant safety standard complies with the other and thus safety artefact reuse consequences. The approach has been validated with practitioners in a case study on the reuse of an execution platform from railway to avionics. To the best of our knowledge, no other approach has been developed in order to systematically reuse safety certification artefacts across standards and domains.

This paper extends the work presented in [17], where we presented an overview of the case study and reported on the experience in mapping EN 50128 and DO-178. The extension is mainly based on: (1) a more detailed explanation of the background, the foundations, and the rationale of the reuse approach; (2) a general and generic description of the principles of the approach and of the process to apply it, indicating and explaining all the necessary activities, and; (3) a deeper presentation and analysis of the validation of the approach, including the reporting and discussion of further results. This extension allows a reader to gain a wider understanding of

how the reuse approach has been developed, its basis, how to apply the approach, and the benefits of its application. Our previous work also just focused on a simple mapping between the two standards and presented a reduced set of metrics for improvement measurement. The current paper presents an extended set of metrics that allows us to provide an analysis of efforts and cost estimation with and without the reuse approach.

The rest of the paper is organized as follows. Section 2 presents the background of the paper. Section 3 describes the reuse approach, and Section 4 reports on its validation. Section 5 summarises our conclusions and future work.

2 BACKGROUND

This section presents the main background of the paper, which corresponds to (1) the current state of the practice, (2) a comparison of safety standards, and (3) the related literature.

2.1 State of the practice

The purpose of this section is to describe how safety-critical system certification is handled in practice. To this end, the section analyses safety certification and reuse in avionics and railway, the two domains addressed in the case study with which the reuse approach has been validated. The comparison of safety standards in the next sub-section complements this analysis by presenting a broader overview of how the standards in further domains are and of their similarities and commonalities.

Certification is defined in civil aviation as a legal recognition that a product, service, organization, or person complies with the requirements stated in a certain standard. This implies technically checking the object of certification to verify formally that it complies with the applicable requirements. For certifying a product, the authority should assess the design process of the product to ensure an acceptable level of safety, check whether the product actually conforms to the expected design, and issuance a certificate required by the national laws to show that the product has gone through the assessments process [3].

Chevrel [18] describes the different actors involved in aircraft manufacturing. First, the aircraft manufacturer agrees with the avionics authority of the country upon the type certificate. This certificate will include the first definition of the product with documents defining the aircraft characteristics. This is done at the very beginning of the design phase. The manufacturer will then make a contract with the different avionics system developers to contract the development of one or more systems of the aircraft and request their contribution to the airworthiness certification process. System development suppliers should also contact with the authority in order to get a Technical Standard Order (TSO) authorization to ensure that their system is compliant with the avionics standards. Getting this authorization does not mean that the system will be certified. The aircraft manufacturer has to discuss with the authority in order to get the authorisation for installing the system on an aircraft. After the installation, the complete aircraft goes through a safety assessment and it is after all the evaluation process that the aircraft is ready to get the airworthiness certification.

In the avionics domain, the DO-297 standard [10] and the advisory circular AC 20-148 [19] deal with reuse. DO-297 appeared as a consequence of the move from federated architectures to IMA (Integrated Modular Avionics) architecture, and AC 20-148 is the result of creating guidelines for software component reuse. AC 20-148 provides recommendations concerning reusable software components. This advisory circular indicates that, to reuse components, stakeholders must identify any possible concern related to installation, safety, operational, functional, and performance. Although AC 20-148 is not a standard, its application is highly recommended when using Reusable Software Components [19]. AC 20-148 distinguishes between what the component is from the developer perspective and from the integrator one. This resembles preconditions and postconditions that should be accomplished for suitable reuse.

IMA is the term used for a distributed computing network aboard aircraft, which supports avionics applications of many different assurance levels, and it is designed for flexibility in configurations and modularity. It supports assurance evidence reuse to reduce effort required when reusing components in different systems. Compliance with DO-297 aims to reduce the cost of maintenance and certification. IMA technology has introduced the possibility to fragment the certification process into several tasks: (a) module and/or platform acceptance; (b) application acceptance (software and hardware); (c) IMA system acceptance (integration of multiple applications); (d) aircraft integration; (e) change of modules or applications; and (f) reuse of modules or applications. IMA aims to enable the reuse of applications from different target systems without increasing the certification costs. The IMA platform architect role establishes a certification baseline about sizing hypothesis (memory, processor throughput), applicable certification standards (e.g., DO-254 and DO-178C), and functionality expected (e.g., ARINC653 API). The module supplier provides what DO-297 calls the usage domain (characteristics and usage constraints and qualification material for certification demonstration).

However, applying DO-297 is not an easy task. Eveleens [20] indicates that one of the challenges of reusing an IMA is the lack of sufficient support for dealing with changes made in existing IMA systems or when reusing design elements. There is a need for justification in order to reuse pre-qualification documents due to the number of acceptance criteria, safety arguments, and evidence that need to be considered in a new integration project.

Regarding railway, the EN 50126 standard [21] covers the specification and demonstration of safety for all railway applications and at all levels of such applications, as appropriate, from complete railway routes to major systems within a railway route, and to individual and combined sub-systems and components within these major systems. This includes software and hardware. The standard also addresses reliability, availability, and maintainability as essential aspects of a railway system that contribute to safety. EN 50126 serves as the entry point or parent standard for other railway standards, such as EN 50128 for software [6] and EN 50129 for electronic systems for signalling [22].

The processes that define the safety lifecycle of a railway system can be tailored, provided that the modifications do not have any consequence on the standard safety lifecycle and are well motivated. For each phase in the design, the activities to be carried out for safety assurance will be executed in parallel. The safety of a system is meant as the property that failure rates of potentially dangerous consequences are low enough, to globally reduce the risk (i.e. the probability of injuries, fatalities, damages) to a specified acceptable value. The process requires the application of EN 50129, which lists factors that influence reliability, availability, maintenance, and safety as defined in EN 50126. The CENELEC Application Guideline (TR 50506-2 [23]) provides additional information on the application of the standard to achieve the case for safety, and includes material concerning Safety Assessment, Safety Approval, and Cross-Acceptance (i.e., reuse).

EN 50129 defines how the conditions for safety acceptance and approval shall be presented. The conditions shall cover three major themes: (1) Quality Management; (2) Safety Management, and; (3) Functional and Technical Safety. The documentary evidence that these conditions have been satisfied shall be included in a structured safety justification document known as the Safety Case. Acceptance by qualified organisations and national regulatory bodies of the Safety Case, through activities of approval, assessment, and cross acceptance, is the ultimate step to allow a railway system to enter passenger service.

2.2 Comparison of standards

Several regulations have been issued for each safety-critical domain. The standards are related to the development, implementation, validation, and maintenance of safety-critical systems. Some examples are:

- IEC 61508 (generic), for functional safety of electrical/electronic/programmable electronic safety-related systems
- ISO 26262 (automotive), for functional safety of road vehicles
- EN 50126 (railway), for the specification and demonstration of reliability, availability, maintainability and safety
- EN 50128 (railway), for software for railway control and protection systems of communications, signalling and processing systems
- EN 50129 (railway), for safety-related electronic systems for signalling of communications, signalling and processing systems
- DO-178C (aerospace), for software considerations in airborne systems and equipment certification
- DO-254 (aerospace), for design assurance of airborne electronic hardware
- SAE-ARP 4754/4754A (aerospace), for development of civil aircraft and systems
- SAE-ARP 4761 (aerospace), for conducting the safety assessment process on civil airborne systems and equipment.

Other standards include IEC 62304, IEC 60601, IEC 14971 for medical equipment, IEC 61513 for nuclear energy, IEC 62061 for industrial machinery, IEC 61511 for industrial processes, IEC 61800 for electronic control motors, and ISO 10218 for robots. Standards are also used in e.g. defence and space.

Since a “common language” for safety is a very long way off, at least a clear understanding of similarities and differences to inform reuse is needed. Different aspects need to be analysed in the standards in order to address the differences and similarities among them. It has to be noted that a deep, comprehensive comparison is out of the scope of this work. However, it is important to understand the most relevant issues.

1) Objectives. Classification of standards can be done based on different criteria.

- *Prescriptive, normative, informative.* Since normative ones are absolutely mandatory, the corresponding domain-specific product needs to comply with that standard. Conversely, the informative ones provide added information and guidance on the use of the aforementioned ones, aiming to facilitate their application.
- *Process-oriented, objectives-oriented, and product-oriented.* Whereas automotive and avionics follow integrated safety, railway prefers the so-called external safety where this attribute is monitored and guaranteed by a different specific system. There are basically two approaches for defining the

implication of safety requirements: objectives-oriented (process-oriented) versus product-oriented. The former specifies requirements implications as objectives, whereas the latter defines constraints on what is possible to observe on an artefact. Project management and independent assessment are process-oriented activities. Hardware and software design or coding rules are usually product-oriented.

2) Terminology/Vocabulary. Although there is some common terminology used across the different safety standards, sometimes their definitions do not absolutely match or even are different from general definitions [51]. It might happen that definitions about common dependability terms such as fault, error, failure, safety, or some other terms like random hardware and systematic faults, are either differently used or even not considered within them. An example to be highlighted concerns to error definition. For example, Laprie defines it as the part of the system state that may cause a subsequent failure [24], whereas DO-178C considers it a mistake in design, code or requirements and a fault its manifestation. Differences also exist in common terms like verification, validation, safety, assessment, and certification.

3) Reuse. The avionics domain uses commercial-off-the-shelf components, which were originally designed for a non-aerospace market. The advisory circular AC 20-148 presents the software component for reuse as a commercial-off-the-shelf component, and DO-297 addresses module or application reuse for IMA platforms. ISO 26262 includes information regarding the safety element out of context, but the guidelines provided are very high-level considerations. It is when dealing with the hardware and software qualified component concepts that we can go deeper into the knowledge of the actual requirements for compliance. IEC 61508 uses another relevant reuse concept, the so-called safety manual for the qualified item.

4) Safety Lifecycle and Safety Management/Lifecycle. There are safety lifecycle similarities and differences with regard to activities related to safety compliance and to the planning of such activities within the system development processes. To start with, some standards define a precise safety management process (e.g., ISO 26262 and IEC 61508), whereas e.g. DO-178C does not and the number of required processes differs. The provision of a safety case (i.e., a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment) is compulsory in railway while highly recommended in other domains.

5) Hardware Development Lifecycle. Some standards such as ISO 26262 consider hardware process and product integrity within the same unique standard, whilst avionics established a separate specific standard (DO-254). ISO 26262 and IEC 61508 include the definition of specific failures rates per integrity level and different hardware metrics to be achieved. Differences can be found not only in the types of faults but also in the hardware metrics to calculate. In automotive, a specific maximum failure rate value per ASIL (Automotive Safety Integrity Level) is established, but this is not defined in all safety standards. Concerning reprogrammable hardware, it is not directly considered in ISO 26262, whereas DO-254 tackles this aspect.

6) Software Development Lifecycle. Not all the safety standards prescribe a specific software development lifecycle. ISO 26262 is one of the standards that explicitly define a V-Model to develop software.

7) Safety Categories or Levels of Integrity. Under various names but addressing the same aim, they constitute a fundamental basis of safety standards. They are called Safety Integrity Levels (SILs) in IEC 61508 and railway, ASIL in the automotive domain, and Development Assurance Level (DAL) in avionics. A given level corresponds to one of several levels (typically four) to determine the item's or element's necessary requirements of the functional safety standard, and the safety measures to apply for avoiding an unreasonable residual risk. In the case of ISO 26262, D represents the most stringent value and A stands for the least stringent level, whereas in avionics it is assigned in the other way around, i.e. A the maximum and D the lowest possible value. All of them depict the risk and the effects of the potential failures of the considered system, making possible to quantify the safety level of a system and consequently to evaluate criticality. Thus it associates a value that characterizes how much the safety depends on the absence of failures from the system under consideration. The higher the integrity level is, the more exhaustive the development and V&V processes need to be so that development faults are avoided as much as possible and random hardware faults are either detected or corrected. This implies that the requirements to comply with increase as the safety level does. This is the case when dealing with specific techniques or methods for a certain design phase. Depending on the criticality level to address, either complementary techniques or more exhaustive ones are needed to comply with the standard (see techniques). Railway and automotive functional safety standards associate a specific SIL/ASIL with a maximum mean time to failure or minimum (dangerous) failure rate. In avionics, there is no attempt to numerically evaluate the probability of failure due to such faults, but to consider that fulfilling standard's requirements provides a level of confidence compatible with the severity of the risk.

8) Hazard Analysis and Risk Assessment (HARA). The hazards related to the safety-related functions are addressed in all the standards following a systematic analysis. According to ISO 26262, HARA is the method to identify and categorize hazardous events of items and to specify safety goals and ASILs related to the prevention or mitigation of the associated hazards in order to avoid unreasonable risk. Furthermore, this standard specifies methods such as FMEA (Failure Modes and Effects Analysis) or brainstorming in order to derive the possible hazards. The impact factors such as severity or exposure used to determine the corresponding integrity levels can

differ to some extent among domains. For example, automotive takes controllability into account, and in avionics severity is implicitly considered as high exposure.

9) Verification and Validation.

As stated in [51], Verification can be defined as the process to check if we are building the system right, guaranteeing that the system has been devised according to the requirements and design specifications. On the other hand, validation is defined as set of activities to see if we are building the right system, thus it ensures that the product meets user's needs. Verification usually stands for the determination of the completeness and correctness of the specification or implementation of requirements from a phase or sub-phase [7]. Even though the definitions might be a bit different among standards, the aim is the same in all of them. Concerning the applied methods, they can differ. Common ones are analysis and review. However, concerning validation, the definition can differ to the previous one and furthermore it does not match between standards. Some such as ISO 26262 considers it as the provision of evidence of the absence of erroneous activation for safety mechanisms, and of compliance to the safety goals. DO-178 defines it as the determination that the requirements are the correct ones and that they are complete. To be more precise, ISO 26262 refers to this term as "safety validation", where methods such as reviews, reproducible tests with pass/fail criteria, or analyses can be applied to assure that the safety goals are sufficient and have been achieved. Validation in IEC 61508 stands for safety validation as well and similar methods are implemented (e.g., testing and static/dynamic analysis). However, DO-178C does not specify any method to be applied and its definition is based on the completeness of the specified requirements.

10) Techniques. The applied techniques or methods do not only depend on the type of standard but also on the criticality level and the product development phase. Furthermore, some techniques can be recommended or highly recommended whereas others are strictly mandatory. Several techniques are usually listed for each development phase. A full mapping of all the required techniques is out of the scope of this work. However, some of the most remarkable are formal methods, FMEA (Failure Modes and Effects Analysis), FMEDA (Failure Modes Effects and Diagnostics Analysis), FTA (Fault Tree Analysis), DFA (Dependent Failure Analysis), testing, walk-through, and simulation. In the case of fault injection, even if it represents a powerful technique for dependability validation and fault tolerance evaluation, no all the selected standards suggest its use. ISO 26262 points it out as a method for validation at system and hardware level while IEC 61508 considers it mandatory for validating fault tolerance mechanisms; Most of the aforementioned techniques appear in different safety standards. Nonetheless, there are similarities and divergences in terms of lifecycle phase, objective and scope, or recommendation level.

11) Tool qualification. Failure to automate complex verification and development activities can compromise system safety. In order to mitigate this risk, integrity requirements in terms of tool qualification can be provided. Most domains have introduced tool qualification requirements concerning planning, documentation, classification analysis, qualification reporting, and confidence, and categorize tools based on the potential impact of it on the application. Regarding requirements on tool development, DO-330 is currently the standard with more elaborated requirements.

12) Security Aspects. Security-related safety issues are starting to be state of the art and something is quite clear: there is no safety without security. However, not all the standards consider security aspects within their requirements, and the trend seems to be the generation of complementary security standards. Railway has already included security aspects in the last version of EN 50129 following an integrative security/safety approach. The same applies to IEC 61508. Its last versions addresses security-aware safety guidelines. In avionics there are also two published standards targeting security issues: DO-326A (airworthiness security process specification) and DO-356 (Airworthiness Security Methods and considerations). To finish with, the SAE (Society of Automotive Engineers) [52] has recently published J3061 based on previous worked performed by National Highway Traffic Safety Administration (NHTSA), [53,54,55,56,57] a cybersecurity guidebook for Cyber-Physical Automotive Systems, consistent with risk methodology in ISO 26262. All of them mainly contain frameworks and processes (including key lifecycle alignment points) and evaluate Threat Analysis and Risk Assessment methods or suggest new safety and security analysis methods to evaluate the safety impact created by security concerns.

2.3 Related literature

Related literature on the reuse of certification artefacts across standards and across domains can be regarded as limited. Nonetheless, some authors have analysed reuse needs and proposed approaches to support artefact reuse. We review this kind of publications in this section.

Reusing artefacts from one domain into others is not a straightforward activity, and it requires a negotiation for its reuse [25]. There are scarce industrial reports describing component reuse such as the one described in [26]. In the software engineering domain, several research works have been focused on reusing components [27,28], architectures [29], and techniques [28,30,31]. Some approaches targeting reuse are also applied in sectors such

as manufacturing [32], where cost-effectiveness of reuse is considered to decide upon reuse. The automotive industry also reuses some parts of their components [33, 34].

Reusing an artefact that has been previously certified in one domain implies a wide and deep analysis for its use in a different domain or project. It is especially relevant when human lives are involved or they might be affected by a misbehaviour or failure of a system. Reusing a project is not straightforward and is even more difficult when the context changes, as for example in cross-domain reuse. This can be a reason of why very few attempts have been made. Zeller et al. [35] propose a cross-domain assurance process in conjunction with a development methodology for safety-relevant software. The objective was to reduce the effort required to perform a safety assessment by reusing safety analysis techniques and tools as well as artefacts produced during the safety assurance process. The process consisted of generic and domain-specific steps that must be executed in each of the considered domains as well as steps that are only necessary in specific domains. The authors were able to reuse techniques and tools for safety analysis on different domains. However, not all of the phases of their proposed process were domain-independent and safety certification artefact reuse was not considered in their research. Papadopoulos and McDermid developed a similar approach [36].

SafeCer (<http://safecer.eu/>) is a European research project related to reuse of safety certification artefacts across standards and domains. The SafeCer project addressed an industrial use case on the reuse of tool qualification across domains [37]. The proposal is based on three pillars: (1) cross-domain requirements spanning different standards, (2) cross-domain development process according to the associated standards and their integrity levels, and (3) cross-domain tools, instantiated according to the associated standard. They proposed a tool qualification process line to enable the reuse across domain of process elements. Gallina et al. [38] stated that this approach also supports the reuse of certification artefacts by relating the process line with the corresponding family of process-based arguments related to process compliance. However, this has not been shown and a systematic process for safety certification artefact reuse has not been specified. Gallina and Szatmári [39] have also proposed the use of ontologies for identification of commonalities and differences among safety processes.

Model-driven approaches can also be applied for certification purposes [40]. New systems can be composed of subsystems stemming from different domains [41], but it is not clear how an artefact can be reused in this context. Some approaches rely on safety cases (thus on arguments; e.g., [42]). However, with these approaches the engineer needs to interpret the requirements and objectives of the standards that will apply to the specific situation and sometimes this is open to interpretations.

3 APPROACH FOR REUSE OF SAFETY CERTIFICATION ARTEFACTS

As explained in the previous section, practices for safety-critical system engineering and assurance vary among domains. There are not only similarities but also differences between the applicable safety standards. Therefore, any approach targeting safety certification artefact reuse must provide a systematic way to check commonalities and identify the differences, and to tackle them. Although recommendations on reuse can be found for some domains, no guidance has yet been provided on how to systematically reuse safety certification artefacts across standards and domains. The related literature has also provided very few insights into how to reuse safety certification artefacts across standard and domains. A new, systematic approach is necessary to reusing safety certification artefacts across standards and domains.

This section presents the approach developed in the OPENCROSS project to reuse safety certification artefacts across standards and domains. We first introduce the overall approach for evolutionary certification of safety-critical systems and then the principles and the process for reuse of safety certification artefacts. Both the principles and the process are supported by the tool platform developed in OPENCROSS [43]. This shows that they can be implemented. We use information from the DO-178C avionics standard [3] and the EN 50128 railway standard [6] as running examples. These standards have been used in the validation of the reuse approach (Section 4). Finally, we discuss practical considerations of the reuse approach.

3.1 OPENCROSS approach for evolutionary certification of safety-critical systems

OPENCROSS is a large-scale European research project on safety assurance and certification of embedded systems. The OPENCROSS consortium comprises four academic partners and 13 companies, including safety-critical system manufacturers, component suppliers, certification authorities, safety assessors, and tool vendors. The project is also supported by a large advisory board with representatives from more than 20 international organizations.

The project has (1) devised a common certification framework that spans different vertical markets for railway, avionics, and automotive, and (2) developed an open-source safety certification infrastructure. The ultimate goal of the project is to bring about substantial reductions in recurring safety certification costs and at the same time reduce certification risks through the introduction of more systematic safety assurance practices. The project deals with: (1) creation of a common certification conceptual framework; (2) compositional certification; (3)

evolutionary chain of evidence; (4) transparent certification process; and (5) compliance-aware development process.

The reuse of safety certification artefacts across standards and domains is mostly enabled by the common certification conceptual framework. The main objective of the framework is to create a language that can be used in different domains to describe safety-related information, standards, and projects. Such a language facilitates the analysis and the comparison of safety standards, and the reuse of safety-related information across projects. This includes projects under different safety standards or in different domain.

Fig. 1 sketches the approach defined in OPENCROSS for evolutionary certification of safety-critical systems. The approach is model-based and is supported by several metamodels targeted at different safety assurance and certification needs. The set of metamodels corresponds to the common certification conceptual framework.

- The Reference Assurance Framework Metamodel supports the specification of the safety compliance needs that have or might have to be considered in an assurance project. The needs can be specified by means of reference assurable elements in the form of reference requirements to fulfil, reference artefacts to manage, and reference activities to execute. Safety compliance needs can be from specific standards, recommended practices, or company-specific practices, and typically have to be tailored to project-specific characteristics. The latter is done by means of baselines, which correspond to the specific safety criteria of a standard with which a given assurance project has to show compliance. A baseline is usually a subset of all the safety criteria present in a standard and varies among projects. For example, the safety criteria will vary if a system is developed using model-based techniques.
- Another source of information for safety compliance is the data about the product for which compliance is sought. Therefore, the metamodels also include the concepts and relationships necessary for modelling and managing project- and product-specific information. This information is referred to as assurance asset and needs to be recorded regardless of which safety standard is being followed. OPENCROSS has defined metamodels for modelling the assurance assets of a project in the form of:
 - The process executed to create a product (Process Metamodel);
 - The evidence of safety and of compliance (Evidence Metamodel), and;
 - The arguments that will be used to justify key safety-related decisions taken during the project (Argumentation Metamodel).

The evidence, in the form of artefacts, can be input and output of the activities of the process and support the arguments. The arguments can refer to process aspects.

- The Vocabulary Metamodel is a means to define and record the terms and concepts used to characterize reusable assurance assets such as evidence, argumentation, and process data. The terms of the vocabulary can thus be used when naming or describing the assurance assets, as well as elements of a reference framework. Terms and concepts of the vocabulary can be specified from the text of a safety standard or be specific to some company, product, or application.
- By using the Mappings Metamodel, maps can be created to specify the degree of equivalence between vocabulary terms (e.g. from different domains), between the assurance information gathered during a project (e.g., artefacts) and its baseline for indicating compliance, and between safety standards (i.e. reference assurance frameworks) for indicating how the standards relate. The latter is a key to reuse of safety certification artefacts across different standards and domains. In general, the mappings aim to allow engineers and managers to make informed decisions about the appropriateness and implications of reusing assurance information across projects, safety standards, and domains.

Further information about the OPENCROSS approach for evolutionary certification of safety-critical systems can be found in [44].

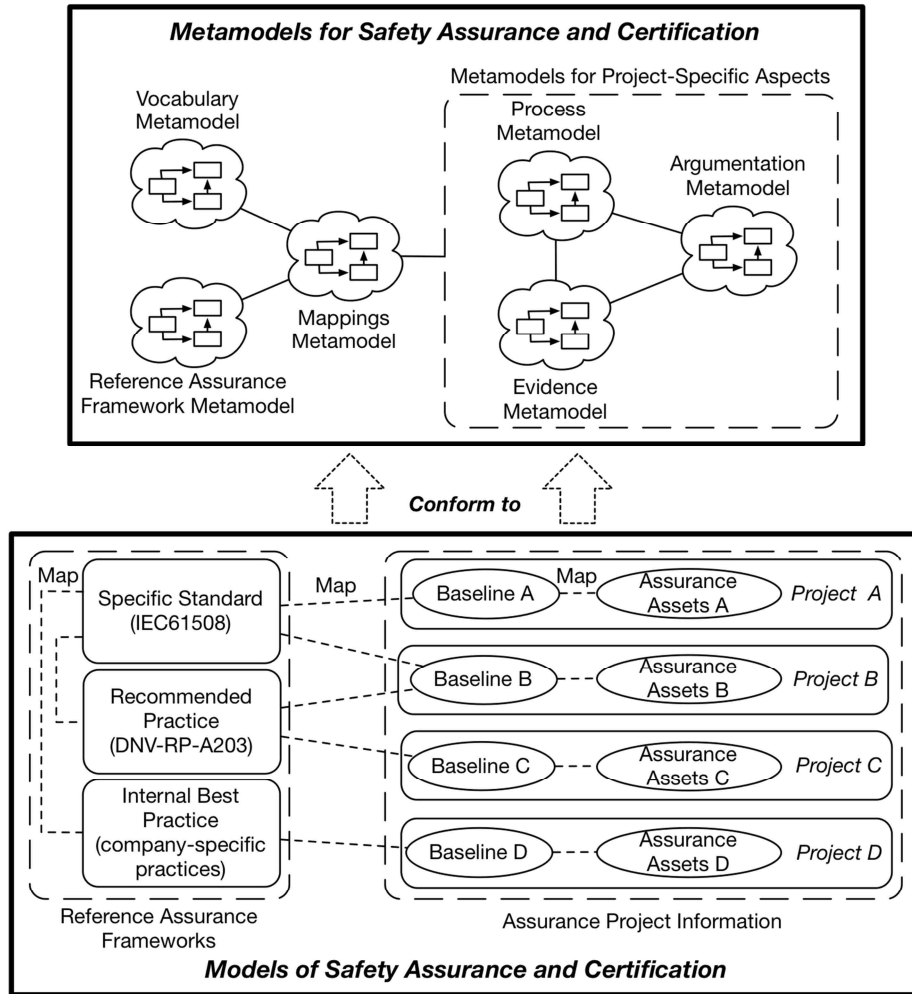


Fig. 1. Overview of the OPENCROSS approach for safety assurance and certification [45]

3.2 Principles for reuse of safety certification artefacts across standards and domains

The application of the reuse approach is based on principles elicited from current practices and needs (see Section 2), and discussed with OPENCROSS industry partners. There are four main principles: the intent of a safety certification artefact must be taken into account when aiming to reuse it, maps must be established between the source standard (*reuse from*) and the target one (*reuse to*), project compliance must be determined (by means of maps), and needs and gaps resulting from safety certification artefact reuse must be determined.

1) Safety certification artefact intent

Safety certification artefact reuse is not a challenge per se. In theory, any artefact is reusable. The main reuse need stems from the fact that each safety standard has its own requirements to fulfil, and such requirements can vary among standards. For example, DO-178C lists objectives (requirements) for the different software development processes, and some objectives are not fully addressed in EN 50128. When reusing a safety certification artefact, it must be determined what requirements of the target standard are fulfilled when the source standard is complied with. Safety certification artefact reuse can be regarded as the process targeted at determining what requirements of a given safety standard are fulfilled when compliance with another standard has been achieved.

The above need can only be met if the standard's requirements to whose fulfilment a safety certification artefact contributes are recorded. These requirements correspond to the artefact intent: what properties are assured in the artefact and thus why the artefact is necessary. For example, the DO-178C Software Requirements Data must include the performance criteria, timing requirements and constraints, and memory size constraints so that the artefact fulfils its intent (i.e., to show that such characteristics have been considered and specified).

Safety certification artefact intent is also based on the activities that use or produce the artefact. In general, and if we think of activities that use and produce several safety certification artefacts, the overall aim of an activity corresponds to a higher-level intent of the individual intent of the output artefacts of the activity. The achievement of this higher-level intent is also enabled by the individual intent of the input artefacts of the

activity. For example, EN 50128 Integration Process (activity) aims to demonstrate that software and hardware interact correctly to perform their intended functions. To this end, the activity uses the Software Integration Test Specification and the Software/Hardware Integration Test Specification as input, and produces the Software Integration Test Report and the Software/Hardware Integration Test Report as output.

2) Equivalence mapping between standards

In addition to recording the intent of the safety certification artefacts, it is also necessary to determine the equivalence between standards for safety certification artefact reuse. This can be done by means of maps that indicate the extent to which the criteria of the standards are equal (e.g., between EN 50128 Software Requirements Specification and DO-178C Software Requirements Data). Based on these mappings, the similarity and differences of the standards can be assessed, and thus how compliant a safety certification artefact is with a given standard according to its compliance with another standard.

Three general types of maps can exist between the elements of two standards:

- *Full map*: the elements in the mapping are identical; the characteristics of the element in its original context (its form, its required content, its preconditions, its objectives, its post-conditions on its use...) fully satisfy the requirements of the context in which it is to be reused.
- *Partial map*: the elements are similar, but they are not identical; depending on the context and the objectives, the differences between them might be significant; in this case, a clear record of the similarities and differences is required.
- *No map*: there is insufficient similarity between the elements to enable us to assert a map; in this case, it may be important to record the differences, and the reasons why the mapping is disallowed, in order to inform further gap analysis and prevent inadvertent reuse.

Full maps are usually rare in the assurance domain and the majority of maps are partial.

Three elements play a role in equivalence mapping: artefacts, activities, and requirements. Pragmatically, any of these reference assurable elements can be reused. The acceptability of the reuse needs to be argued in terms of the overall assurance objectives indicated by a standard: i.e. what needs to be demonstrated for assurance and compliance in the target context.

Equivalence maps are also necessary between the baseline of an assurance project and the reference framework (or frameworks) of the standard according to which a system has to be assured. Some differences might exist as result of e.g. having to tailor how to follow a standard according to the specific characteristics of a system.

3) Compliance mapping

Another necessary type of maps for cross-standard and cross-domain reuse is compliance maps. These mappings specify how the information of an assurance project (i.e., its body of assurance assets) complies with its baseline. As equivalence maps, compliance maps can be full, partial, or no map. By mapping an artefact to a reference artefact selected for a baseline, the intent of the artefact is indicated.

The compliance maps of the source assurance project will typically be full and 1:1. Its baseline will correspond to a template according to which the project is executed. For example, a baseline from a reference framework for DO-178C will have Software Requirements Data as an artefact to provide, and an assurance project can have a single artefact that maps to Software Requirements Data. Nonetheless, an assurance project can also manage, structure, or group its artefacts in a different way to what a standard indicates, but still being compliant. For example, an assurance project could have more than one artefact for its Software Requirements Data, such as high-level requirements specification and low-level requirements specification. Each of these artefacts would partially map to Software Requirements Data.

Compliance maps for the target assurance project can be derived from the compliance maps of the source project. In this case, the likelihood of derived full maps is low because of the differences that usually exist between standards. The assurance information of the source project fulfils the requirements of its baseline and it turn of some source reference framework. The target assurance project will have a different baseline and reference framework, thus different requirements to fulfil. Nonetheless, some reference requirements can be similar or equal. For example, an artefact that complies with EN 50128 Software Requirements Specification will partially map to DO-178C Software Requirements Data.

4) Needs and gaps from safety certification artefact reuse

Finally, reuse of safety certification artefacts across standards and across domains requires that compliance needs and gaps resulting from the reuse are determined. This is a consequence of the fact that the maps between standards are most often partial. Compliance with a standard will allow a system to comply with another to some extent, but fulfilment of further reference requirements for the target project will be necessary. This will usually involve the execution of some activity or the creation of some artefact.

For example, reusing EN 50128 Software Requirements Specification in an avionics assurance project will lead to the partial fulfilment of the reference requirements for DO-178C Software Requirements Data. The corresponding compliance gaps must be filled for full compliance with DO-178C.

3.3 Process for reuse of assurance assets across standards and across domains

The process developed in OPENCROSS to apply the reuse approach is part of the project's overall approach for evolutionary certification of safety-critical systems (Section 3.1). The process consists of seven main activities and is based on the conceptual framework shown in Fig. 2. This framework corresponds to excerpts of all the metamodels created in OPENCROSS [44]. All the attributes and associations of the conceptual framework are not shown to keep the figure as small and simple as possible, and so that it focuses on the main aspects of the reuse approach. Although presented as a sequence, some activities of the process can be executed in parallel, iteratively, or in a different order. For example, the baseline of an assurance can be modified while collecting assurance assets because of some new request by a safety assessor.

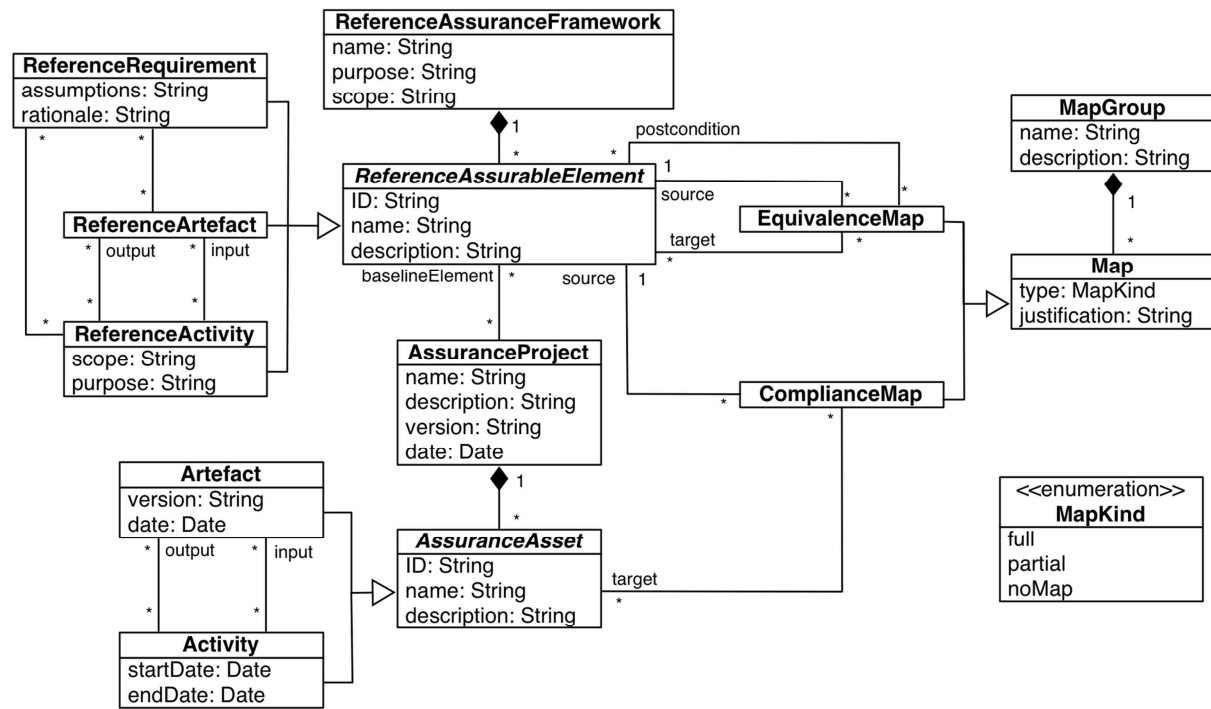


Fig. 2. Reuse conceptual framework

1) Create reference assurance frameworks

The first activity to apply the reuse approach is to specify the compliance needs of the standards to comply with in the source and the target domains. A reference assurance framework must be created for each standard, and the frameworks will be later used for specifying baselines and equivalence maps.

The reference frameworks will contain reference requirements to fulfil, reference activities to execute, and reference artefacts to manage. Reference artefacts can be linked to reference requirements and to reference activities (input/output), which enables the specification of reference artefact intents. In EN 50128, Software Design Specification is a reference artefact, Component Design is a reference activity, and “test cases and their results shall be recorded, preferably in machine readable form for subsequent analysis” (clause 7.6.4.5.a) is a reference requirement for the Software Integration Test Report. Reference artefacts, activities, and requirements can be decomposed into others.

A reference framework can further contain information about the reference roles that might be involved in a safety-critical system's lifecycle (e.g., designer), the reference techniques that might be used to execute reference activities and create reference artefacts (e.g., formal methods), and applicability of the above elements (e.g., a given reference technique can be recommended for a given SIL in EN 50128). A reference artefact can also have reference artefact attributes (e.g., test outcome; passed or failed) and be linked to other reference artefacts by means of reference artefact relationships (e.g., Design Description satisfies Software Requirements Data).

More information about reference assurance frameworks, how to create them, and their usage can be found in [45].

2) Specify equivalence maps between the reference assurance frameworks

Once reference assurance frameworks have been created, equivalence maps can be specified between their reference assurable elements in order to determine how similar the frameworks are. Each equivalence map will

have a source and a target reference assurable element, can have a textual justification, and can have postconditions. The postconditions correspond to additional reference assurable elements that must be taken into account when an artefact is reused.

When creating equivalence maps for safety certification artefact reuse (i.e., between reference artefacts), and as explained above, it is essential to analyse the intent of the reference artefact to decide upon the extent to which two reference artefacts are similar. Arguing about the (relative) equivalence between reference artefacts requires discussion of the similarity of the associated reference requirements and reference activities.

The equivalence mapping process might not result in 1:1 maps between e.g. single reference artefacts. A set of source reference artefacts might map as a whole to a single target reference artefact. It can also be necessary to map different types of reference assurable elements. For example, there may be cases where no mapping can be asserted between a reference requirement of the target reference assurance framework and any of the reference requirements of the source, but that the former reference requirement could be mapped to some reference artefact in the source. For the two cases described in this paragraph, the specification of a map justification is especially important to document why the corresponding maps have been specified.

Another aspect to take into account is map consistency. For example, if the reference requirements of a reference artefact partially map to the reference requirements of another referent artefact from a different reference assurance framework, then the map between the reference artefacts must be partial.

As an example, EN 50128 Software Requirements Specification partially map to DO-178 Software Requirements Data because their reference requirements, thus what can be assured with them, are different.

3) Determine the baseline for the source assurance project

The specific compliance needs of the source assurance project must be specified. To this end, the applicable elements of a reference assurance framework must be selected. It is also possible to refine the elements to project-specific needs or to specify information that it is not in the reference assurance framework. For example, DO-178C does not define roles for assurance projects, but such roles might have to be declared for a specific role. When refining a reference assurance framework into a baseline, the suitability of the changes introduced for the corresponding assurance project, in relation to how the baseline corresponds to the reference assurance framework, might need to be justified. This is done by specifying equivalence maps between the baseline and the reference assurance framework.

4) Collect the assurance assets of the source assurance project

The information of the assurance assets of the source assurance project must be collected in order to demonstrate how system safety has been assured. For reuse purposes, the main assurance assets to collect are the artefacts created during system lifecycle. Other assurance assets include the information about the activities executed, the participants in the assurance project, the techniques used, and the argumentation claims. More information about the possible assurance assets of an assurance project and the information to collect about them can be found in [44].

As presented in Section 4 below, a configuration management plan, a system requirements specification, and a validation report are examples of artefacts (assurance assets) about which information can be collected for a railway assurance project.

5) Specify compliance maps between the assurance assets of the source assurance project and its baseline

Compliance maps must be specified for the source assurance project in order to indicate how the project meets its compliance needs. The assurance assets of the project are mapped (full or partial map, or no map) to its baseline, and a justification for the map might be specified.

6) Determine the baseline for the target assurance project

This activity is the same as (3) but for the target assurance project instead of for the source one.

7) Reuse assurance assets from the source assurance project to the target one

Finally, assurance assets from the source assurance project are reused in the target one, for the baseline specified in activity (6). The reuse can result in additional compliance needs for the target assurance project according to the postconditions of the equivalence maps. These needs will be included in the baseline of the target project.

Reuse of assurance assets results in the generation of compliance maps for the target assurance project. This is based on the chain of maps consisting of the compliance maps for the source assurance project and of the equivalence map between reference assurance frameworks, including possible maps between a baseline and a parent reference assurance framework. If there is some partial map in the chain, then the resulting compliance map for the target assurance project will be partial. It might also be necessary to address some postconditions, and it is also essential to analyse the map justifications in order to determine what compliance needs must still be addressed in the target assurance project. When all the maps are full, then the derived compliance map is full too. If there is any 'no map', then the reuse is not advisable. This means in practical terms that no reuse is possible.

For assurance asset reuse between projects, mapping reference requirements can suffice because the reuse consequences can be determined from the correspondence between reference requirements. These consequences can correspond to the need for assuring further reference requirements in the target assurance project.

3.4 Discussion

This section discusses practical considerations for applying the reuse approach.

The first aspect of which a reader must be aware is that the reuse approach focuses on product compliance. Compliance is a requisite for certification, but not the only aspect to address. Compliance does not imply that a system can be deemed safe but that its lifecycle conforms to some standard. It is also necessary to demonstrate that product hazards have been mitigated or avoided for safety assurance. In this sense, and using argument types as a basis [46], the reuse approach deals with the compliance argument of a product, but the technical argument, which justifies risk reduction, is also necessary. A confidence argument that justifies the suitability of the other two arguments might also be necessary. In this sense, product technical aspects must always be taken into account in reuse, such as its operational conditions. These aspects have been addressed in other approaches (see Section 2), and we have focused on compliance reuse across standards and domains.

A major need of the reuse approach is the agreement upon the maps, especially upon equivalence maps. It is not realistic to think that a single person can decide upon them. Several people will usually be required, mostly experts from the domains for which reference assurance frameworks are mapped. They will need to discuss e.g. the extent to which reference requirements are similar, thus the map types, the map justifications, and the postconditions. Agreements upon maps with certification authorities might also be necessary.

It must also be noted that equivalence maps are not bi-directional. The maps from a reference assurance framework to another will usually not be the same as the maps from the latter to the former. For example, if the reference requirements of a reference artefact (1) includes but also extends the reference requirements of another reference artefact from a different reference assurance framework (2), then the equivalence map from (1) to (2) will be full but the map from (2) to (1) will be partial.

Another advantage of equivalence mapping is that the resulting maps can be reused. Once specified, the maps can be used in as many projects as necessary. Although equivalence mapping requires some effort, the return on investment will increase every time the reuse approach is applied.

Finally, the application of the reuse approach will only be possible if the corresponding certification authority agrees upon how it has been applied. This implies an agreement upon the maps specified, including their justification and postconditions. The agreement strongly depends on a thorough and reasoned application of the reuse approach.

4 Case Study

This section describes how the reuse approach has been benchmarked in the OPENCROSS project. The benchmark has consisted of a case study that has analysed the reuse of an execution platform from railway to avionics. OPENCROSS industry partners participated in the benchmark. We also received regular feedback on the reuse approach from OPENCROSS industrial stakeholders (e.g., at project meetings) and its advisory board, which include assessors and certification authorities.

The following subsections introduce the case study, describe how data was collected, present the case study process, and discuss the results.

4.1 Case study description

The case study for benchmarking the reuse approach corresponds to a situation in which an execution platform (computing unit and operating system) developed in the railway domain aims to be qualified in the avionics domain. This platform is considered as a feasible component for reuse; however the objectives and requirements for compliance differ between the domains from the qualification point of view. These differences make it hard to reuse the qualification-related artefacts. It is common to have to redo all or most the qualification activities again in order to produce adequate material for the target domain. The purpose of this reuse scenario is to build the avionics qualification dossier, based on the artefacts provided with the reused parts, without or with limited rework. The qualification dossier is then presented for certification. The execution platform is considered as an independent item that aims avionics DAL B.

The execution platform is considered as an independent item for which a qualification dossier will be built. This qualification dossier consists of plans, technical documents, and certification documents. The technical documents are specifications, validation, and verification data. The certification documents are the configuration index documents and accomplishment summaries.

The initial execution platform and the associated documentation issued from the railway domain comply with EN 50128. The final execution platform and the elaborated qualification documentation to be used in avionics must comply with DO-178C. Figure 3 shows the targeted area of credit in the light of the full certification process. The reuse will occur within a same company with different units for each domain. The company has

processes that are common to all its units, and each unit specialises the processes according to domain-specific needs. This specialisation also includes the tailoring of the applicable standards to the projects of the company.

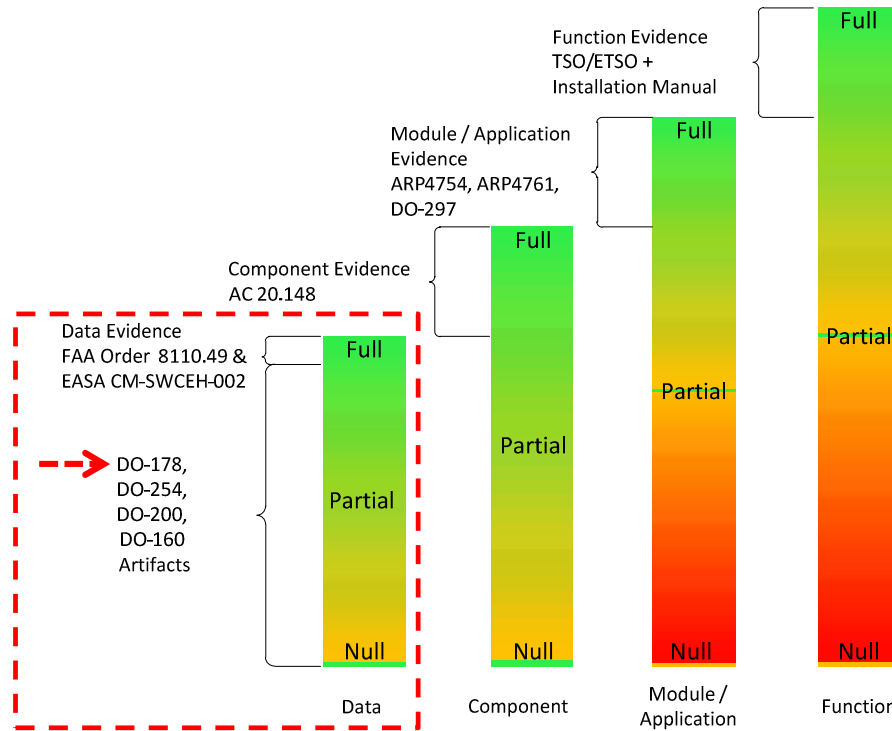


Fig. 3. Targeted area of credit (in red dashed lines)

The overall goal of the case study was to demonstrate a potential reduction of recurring costs for product safety certification across standards and domains. To this end, we formulated the following research questions (RQs).

RQ1. Can the proposed approach be effectively applied to reuse safety certification artefacts?

This RQ aimed at showing that the reuse approach is a feasible and suitable way to reuse safety certification artefacts across standards and applications. If we do not show that the approach can be applied in a realistic scenario with real project data and meets industry expectations, then practitioners will be reluctant to using it.

RQ2. What is the impact of applying the proposed approach to reuse safety certification artefacts?

This RQ aims at showing that the reuse approach is not only effective but also efficient. Whereas RQ1 is a prerequisite for achieving the case study goal, RQ2 answer will allow us to show if the goal is actually achieved. It is essential that we demonstrate the potential reduction of recurring costs so that practitioners find substantial benefits in the application of the approach, when compared to the current state of practice. Showing that the approach is effective would not be enough to raise industry interest and make an impact in the current practices.

4.2 Case Study Process

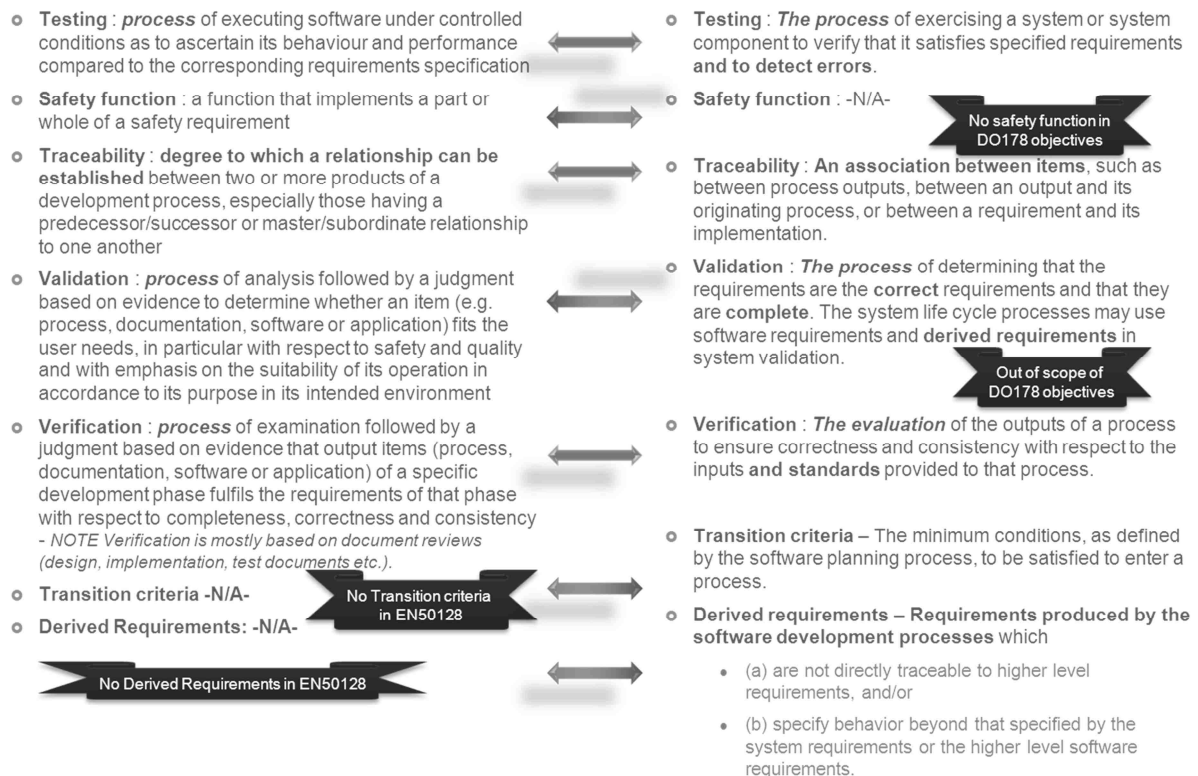
For the case study we have followed the process for reuse of assurance assets presented in Section 3.3.

1) Creating reference assurance frameworks

Before starting to capture an interpretation of the targeted industrial standards, one of the first activities performed was the compilation of a multi-domain and heterogeneous team of experts on airworthiness certification and railway certification. The experts worked on a conceptual understanding of those standards and their equivalences. As a result, there was a series of key conclusions that drove the subsequent activities. Figure 4 summarizes the main equivalence conclusions. In addition, some general findings are as follows:

- Railway standards require specific design features on the products or systems (*prescriptive product-based standards*), while avionics standards specify the process to be used in producing the specific products or systems (*prescriptive process-based standards*).
- Validation in avionics is an Aircraft/System (A/S) dedicated process and a part of ED79A /ARP4754A.
- Safety function in railway is the equivalent of avionics safety-related functions at A/S definition level.
- Validation in avionics is an A/S dedicated process and a part of ED79A/ARP4754A.

- Transition criteria are an important asset for the avionics domain, based on process control demonstration. A general model for avionics safety standard can be provided by similarity with a control loop, double and reversed, which enables to oversee the quality of the design process, including the achievement of the intended function and evidence of compliance associated.



(a) EN 50128 Standard

(b) DO-178C Standard

Fig. 4. Some key conclusions of the conceptual comparison between EN 50128 and DO-178C standards

The next activity was to capture the targeted standards as reference assurance framework models. Figure 5 illustrates a graphical view of EN 50128. This view shows only some of the elements of the standards, i.e. activities, artefacts, and roles. Further information such as reference requirements can be only viewed in tree and form views. Figure 6 shows an excerpt of a recommendation table from EN 50128, both as documented in the standard and as captured in the OPENCROSS tools. It must be noted that all the elements from the standards are captured in a structured view, including criticality levels (e.g. SIL), techniques/methods, applicability levels, and the associated standard's requirements. A similar modelling process was done for DO-178C.

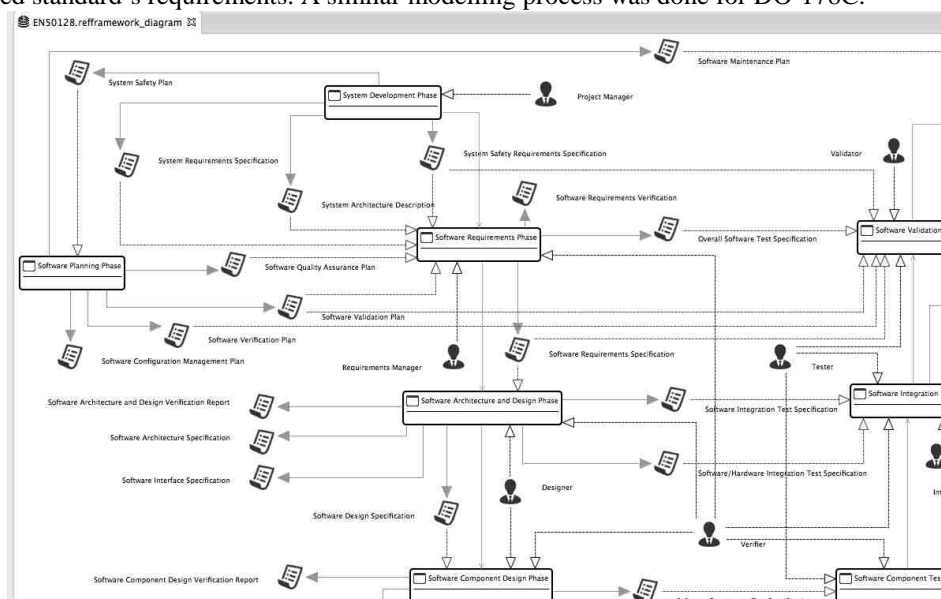


Fig. 5. Excerpt of graphical model of EN 50128 activities, artefacts and roles

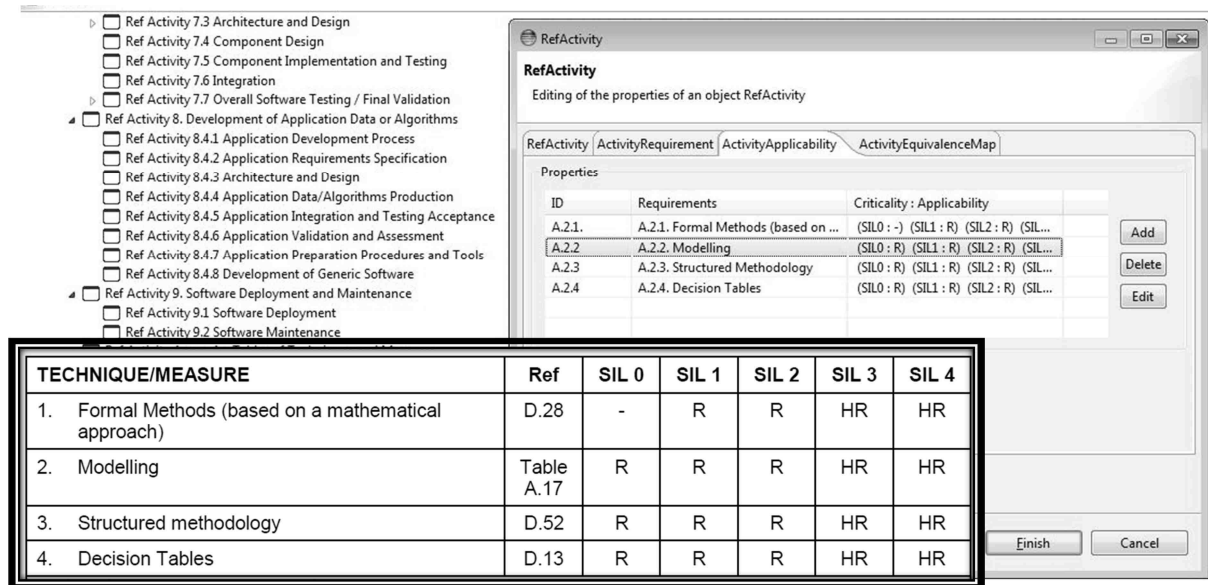


Fig. 6. Excerpt of recommendation table for EN 50128

2) Specify equivalence maps between the reference assurance frameworks

As a prerequisite to assist the reuse activities with OPENCOS tools, the railway and avionics experts captured the equivalence between EN 50128 and DO-178C in the form of equivalence mappings. This includes (a) the identification of links between reference artefacts, requirements, activities, roles; and (b) the identification of “orphan” links in the source industrial standards (i.e. EN 50128) by means of postconditions attached to equivalence maps.

For instance, reusing EN 50128 Software Requirements Specification into a DO-178-based assurance project resulted in the partial fulfilment of the reference requirements for the artefact(s) that corresponds to DO-178 Software Requirements Data. DO-178 deals with bi-directional association between system requirements allocated to software and high-level requirements (reference requirement on traceability), but EN 50128 only deals with traces from software requirements to the system requirements. Therefore, these reference requirements should be addressed for DO-178 compliance and were modelled by using postconditions. Figure 7 shows an excerpt of the EN 50128 to DO-178C equivalence mapping. A map justification field can be used to document any additional consideration of equivalence.

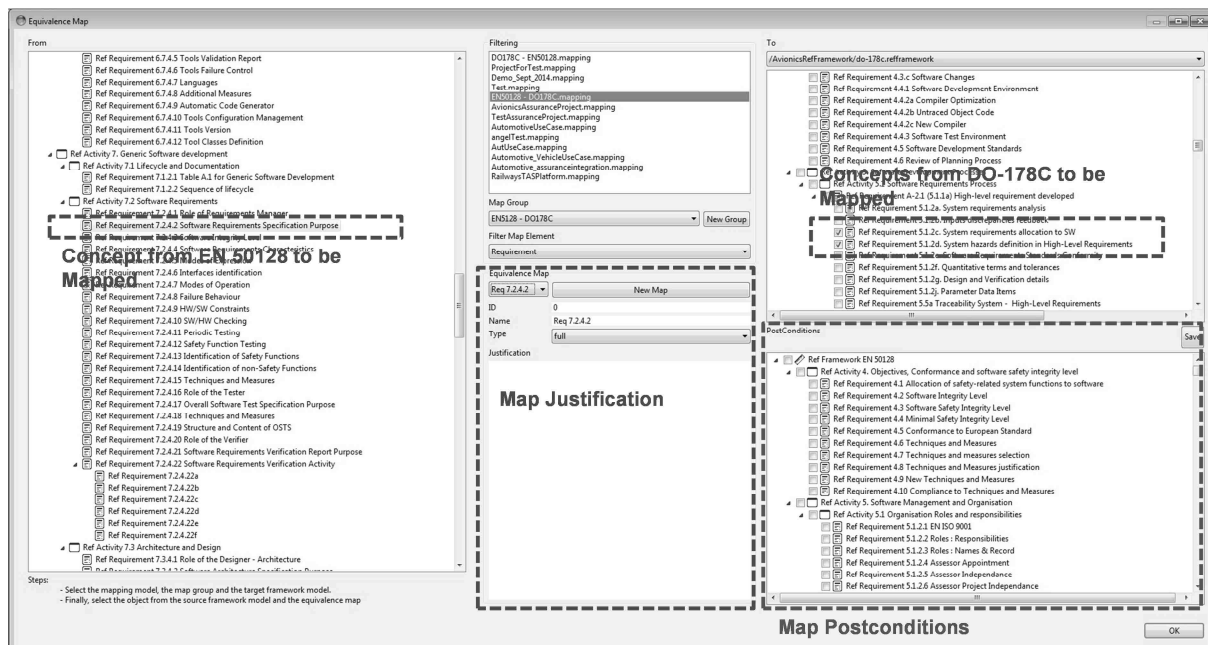


Fig. 7. Modelling of Equivalence Mapping between EN 50128 and DO-178C

3) Determine the baseline for the source assurance project

The previous activities are project-independent in the sense that various projects can use the reference frameworks and equivalence mappings modelled. When working in specific projects, the first step is to create a new assurance project and to define the baseline framework. In order to create the baseline framework, we tailored the railway reference framework (i.e. EN 50128) into a baseline model which represented the compliance obligations for railway assurance project.

4) Collect the assurance assets of the source assurance project

We used the following 28 source artefacts from the railway project:

- Project Management Plan
- Configuration Management Plan
- Documentation Plan
- Quality Management Plan
- Quality Management Plan Reports
- Verification Plan
- Validation Plan
- Handbook of Methods
- Coding Rules for C
- Software Techniques and Measures
- Application relevant problem reports
- Release Notes
- System Requirements Specification
- System Requirements Specification - Safety
- Feature List
- Requirements Traceability Matrix
- Subsystem Requirements - Safety
- Subsystem Requirements - Operating System
- Top Level Architecture
- Detailed Design Document - Operating System
- Detailed Design Document - Compact Flash
- Test Design Specification - System Level
- Test Design Specification - Operating System Level
- Verification Report
- Validation Report
- Validation of Requirements
- Validation report C90
- Test Report - Operating System

These artefacts were modelled in OPENCROSS tools so that all the applicable life cycle data was identified in the tool as a reference for compliance to the standard requirements. Further details about the collected data can be found in [48].

5) Specify compliance maps between the assurance assets of the source assurance project and its baseline

We created compliance maps between baseline model elements and assurance assets elements (e.g. artefacts). For the railway assurance project, the whole set of base artefacts have full compliance maps, since this project accomplished all the obligations in order to be certified.

6) Determine the baseline for the target assurance project

The first step for creating the avionics assurance project was to tailor a baseline model for DO-178C. The avionics experts performed a similar activity as (3) but for the avionics assurance project.

7) Reuse assurance assets from the source assurance project to the target one

Using the “cross-domain reuse” functionality of the OPENCROSS tools allows users to automatically create a folder of avionics project artefacts by using the DO-178C life-cycle structure. Fig. 8 shows a screenshot of how the OPENCROSS tool support for this functionality. The top area provides information about the equivalence between two reference assurance frameworks, whereas the bottom provides information about the reuse consequences. These consequences are based on the artefact from the source assurance project selected for reuse. In this figure, the left side of the screen represents the DO178C project tree with the standard requirements on the top-left side and the automatically-built life cycle data on the down-left side.

Further information about the OPENCROSS tool platform, including details and screenshots about the rest of activities are supported, are available in [43].

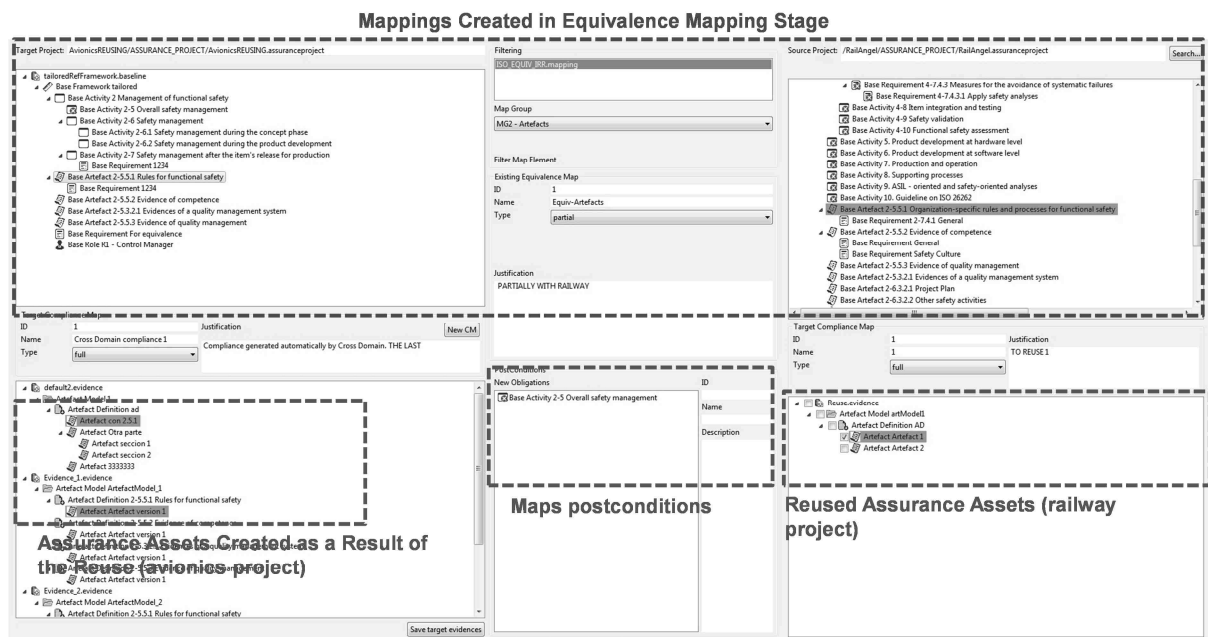


Fig. 8. OPENCROSS tool support for the reuse approach

4.3 Evaluation framework

An evaluation framework and metrics were specified to benchmark the reuse approach, as well as the rest of OPENCROSS results, and thus to answer RQ2. The framework is based on the Goal-Question-Metric approach, aims to support the comparison of safety certification scenarios with and without OPENCROSS results, and was validated by OPENCROSS partners. For the cross-domain reuse case study, the goal that drove the specification of its evaluation framework has been introduced in Section 4.1 (i.e., reduction of recurring costs). The questions and metrics used in the case study to analyse the achievement of the goal were:

1. How can the safety assurance process be efficient for delta demonstration?
 - a. Ratio of assurance assets that are reused
 - b. Ratio of baseline elements that do not need a new compliance map
 - c. Ratio of reference assurable elements with applicable equivalence maps
2. How can automation of the safety assurance process contribute to cost decrease?
 - a. Ratio of compliance maps automatically created
3. How can safety assurance be reused across domains?
 - a. Ratio of reference assurable elements with some equivalence map
 - b. Ratio of assurance asset reuse that are reused across domains (adaptation of metric 1.a for cross-domain)
4. How can awareness of the work necessary for reuse contribute to cost decrease?
 - a. Ratio of baseline elements whose compliance with has to be shown (1 - metric 1.c)

The value of the metrics is between 0 and 1. Further information about these questions and metrics, including their rationale, and about the rest of elements of the OPENCROSS evaluation framework is available in [49].

The metrics can also be used as basis for estimating effort and cost reduction. For the case study, we discussed the metrics with four practitioners (certification managers) and asked them to provide an estimation of the reductions in the following activities:

- Interpretation of safety standards for cross-domain reuse (e.g., equivalence mapping)
- Assurance project configuration (e.g., awareness of reuse consequence)
- Interaction with assessors and certification authorities (e.g., agreement upon compliance means)
- Evidence collection (e.g., evidence reuse)
- Communication to all the stakeholders, including suppliers, customers, assessors, and regulators (e.g., definition of a common understanding of compliance needs)
- Development of accomplishment summaries (e.g., compliance mapping)
- Other safety certification activities (e.g., audit of engineering tasks)

4.4 Results

The main results from applying the reuse approach process (Section 3.3) are summarised in Table 1. Practitioners validated all the results (i.e., the reference assurance frameworks created, the maps specified, etc.). Insights gained from mapping EN 50128 and DO-178 are presented in [17,50]. For example, there is no equivalence for EN50128 software deployment and maintenance in avionics at DO-178C level.

Table. 1. Case study results summary

Process activity	Main Results
1) Create reference assurance frameworks	Reference framework for EN 50128 with 2500+ elements, including 439 reference requirements, 58 reference activities, and 38 reference artefacts Reference framework for DO-178C with 1500+ elements, including 355 reference requirements, 54 reference activities, and 24 reference artefacts
2) Specify equivalence maps between the reference assurance frameworks	256 equivalence maps from EN 50128 reference assurance framework to the DO-178C one
3) Determine the baseline for the source assurance project	Baseline from for railway assurance project with 577 elements selected from the EN 50128 reference assurance framework
4) Collect the assurance assets of the source assurance project	28 artefacts collected
5) Specify compliance maps between the assurance assets of the source assurance project and its baseline	266 compliance maps for the railway assurance project
6) Determine the baseline for the target assurance project	Baseline for avionics assurance project with 611 elements selected from the DO-178 reference assurance framework
7) Reuse assurance assets from the source assurance project to the target one	28 artefacts reused and 155 compliance maps generated for the avionics assurance project

Table 2 shows the value of the evaluation metrics and how they were measured. Metric measurement focused on reference requirements of the baselines. Practitioners suggested this, and it allowed us to more accurately determine the impact of the reuse approach. The number of e.g. artefacts (as assurance assets) was much lower than the number of reference requirements that could be used for metric measurement, and the use of these requirements as basis is suitable because they correspond to the artefacts' intent. In addition, using e.g. reference artefacts as single basis would have been misleading because some map typically exists for all the reference artefacts of a reference assurance framework. This resulted in metric measurement based on intent reuse, which arguably represents assurance reuse more faithfully.

Regarding the estimated effort and cost reductions, Table 3 and Table 4 show the estimates made by the practitioners, where AP1 and AP2 refer to two different assurance projects. A base effort of 100% and a base figured cost of 1M EUR were used. It was also estimated the extent to which the reuse approach covered the activities analysed. The estimates for AP1 with the reuse approach, in which only some aspects would be exploited (e.g., specification of reference assurance frameworks), are based on AP1 without the approach and its coverage. The estimates for reuse from AP1 to AP2 with the reuse approach is based on AP1 with the reuse approach, the coverage of AP1 without the approach, and on reuse from AP1 to AP2 without the approach. Based on the estimates by the practitioners, cross-domain reuse (i.e., Reuse from AP1 to AP2) with the current practices results in only 4.5% of effort and cost reduction. The application of the reuse approach could lead to effort reduction by 53.8% and cost reduction by 26.6%,

Table. 2. Metric measurement

Metric	Value	Comments
Ratio of assurance assets that are reused	0,74	Focused on (reference) baseline requirements

Reused assurance assets	155	Reused compliance requirements
Total assurance assets	210	Total set of avionics baseline requirements
Ratio of baseline elements that do not need a new compliance map	0,19	Focused on (reference) baseline requirements
Baseline elements that do not need a new compliance map	40	Number of assets reused whose compliance map is full
Total baseline elements	210	Total set of reference requirements
Ratio of reference assurable elements with applicable equivalence maps	0,67	Focused on reference requirements
Reference assurable elements with applicable equivalence maps	210	Number of reference requirements with equivalence maps
Total reference assurable elements	315	Total set of reference requirements
Ratio of compliance maps automatically created	0,74	Focused on automated compliance maps for baseline requirements
Compliance maps automatically created	155	
Total compliance maps	210	
Ratio of reference assurable elements with some equivalence map	0,67	Focused on reference requirements
Reference assurable elements with equivalence maps	210	Number of reference requirements with equivalence maps
Total reference assurable elements	315	Total set of avionics reference requirements
Ratio of assurance asset reuse that are reused across domains	0,74	Focused on (reference) baseline requirements
Assurance assets reused across domains	155	Reused compliance requirements
Total assurance assets	210	Total set of avionics baseline requirements
Ratio of baseline elements whose compliance with has to be shown	0,81	Focused on (reference) baseline requirements
Baseline elements that need a new compliance map on the new domain	170	Number of assets that need a compliance map, full or partial, in the new domain
Total baseline elements	210	Total set of avionics compliance requirements

Table. 3. Effort and cost estimation without the reuse approach

Activities	API		Reuse from API to AP2		Coverage of API	
	% Effort	Cost (K€)	% Effort	Cost (K€)	% Effort	Cost (K€)
Interpretation of safety standards for cross-domain reuse	20%	200	18,50%	185	45,00%	90,00
Assurance project configuration	15%	150	14,00%	140	45,00%	67,50
Interaction with assessors and certification authorities	8%	80	8,00%	80	35,00%	28,00
Evidence collection	18%	180	17,50%	175	40,00%	72,00

Communication to all the stakeholders	14%	140	13,50%	135	35,00%	49,00
Development of accomplishment summaries	12%	120	11,00%	110	65,00%	78,00
Other safety certification activities	13%	130	12,00%	120	24,00%	31,20
Total	100%	1.000,00	94,50%	945,00	41,57%	415,70

Table. 4. Effort and cost estimation with the reuse approach

Activities	AP1			Reuse from AP1 to AP2			
	% Effort reduction	Covered cost (K€)	Total cost (K€)	% Effort reduction	Covered cost (K€)	Total cost (K€)	% Cost reduction
Interpretation of safety standards for cross-domain reuse	30,00%	63,00	173,00	67,00%	20,79	122,54	33,76%
Assurance project configuration	15,00%	57,38	139,88	81,00%	10,90	87,90	37,21%
Interaction with assessors and certification authorities	18,00%	22,96	74,96	19,00%	18,60	70,60	11,75%
Evidence collection	18,00%	59,04	167,04	74,00%	15,35	120,35	31,23%
Communication to all the stakeholders	18,00%	40,18	131,18	5,00%	38,17	125,92	6,73%
Development of accomplishment summaries	60,00%	31,20	73,20	74,00%	8,11	46,61	57,63%
Other safety certification activities	5,00%	29,64	128,44	5,00%	28,16	119,36	0,53%
Total	11,23%	303,40	887,70	53,83%	140,08	693,28	26,64%

4.5 Discussion

We discuss in this section the answers to the RQs, the practical considerations for applying the reuse approach, and the validity of the results obtained and the conclusions drawn.

We consider that the answer to **RQ1** (Can the approach be effectively applied for reuse of certification artefacts?) is positive. The results of the case study, which were validated by practitioners, show that the reuse approach was successfully applied for analysing the reuse of an execution platform from railway to avionics. All the activities of the process to enact the approach (Section 3.3) could be executed, and in accordance to the reuse principles presented (Section 3.2). The whole set of artefacts from railway could be reused and the reuse consequences could be determined.

When analysing the impact of applying the proposed approach (**RQ2**), the results strongly suggest that the reuse approach can reduce recurring costs for product safety certification across standards and domains. First, metric measurement shows gains above 65%, with almost a 20% of baseline elements that do not need new compliance maps (i.e., already compliant elements after reuse). Second, practitioners consider that the application of the reuse approach can lead to effort reduction above 50% and to cost reductions above 25%. Even though the estimates were too optimistic, we consider that the estimates provide evidence of the potential effort and cost reductions that the reuse approach can enable.

There are aspects related to the **validity** of the case study that are inherent to this research method, such as the application of the approach in a single case and in a given context (reuse of an execution platform from railway to avionics). This affects external validity. Other aspects of which a reader must be aware are as follows:

- Fully accurate results can only be obtained if the reuse approach is applied a real full project. The current validation has been the initial step towards demonstrating the potential of the approach in practice.
- Some results are based on estimates. This has been mitigated by taking measures to provide sound estimates (e.g., involvement of several practitioners).
- The case study has focused on the reuse between two software standards. The results might thus differ for e.g. system-level standards. The same applies to reuse situations in which goal-based standards are involved and assurance projects that have to show compliance with several standards.

Nonetheless, we are confident in the overall validity of the case study, thus of the reuse approach. First, practitioners have been strongly involved throughout the case study. They also provided regular feedback during OPENCOSS on how the reuse approach should be to fit industry needs. Second, according to the background of the participants of recent large surveys on safety evidence management [13,14], most practitioners involved in safety-critical systems engineering and certification deal with DO-178, EN 50128, or similar standards (e.g., ARP4754 or IEC 61508-based standards, respectively).

5 Conclusion

Product reuse is a common activity in the development of safety-critical systems. It can improve safety-critical system engineering and certification, and there is guidance for product reuse across systems of a same domain. However, reuse across standards and domains has received little attention and no recommendations exists for such reuse scenarios. Although similarities might exist between domains, reusing safety certification artefacts from one domain to another is not a straightforward because each domain has its engineering practices and standards.

This paper has presented a systematic approach to effectively reuse safety certification artefacts across standards and domains. The reuse approach is based on the mapping of the safety criteria of two standards and the mapping of the artefacts of an assurance project to the standard with which the project has to comply. The resulting chain of maps can be later used to identify the consequences of reusing safety certification artefacts from a source assurance project to a target project in another domain and with different applicable standards.

The reuse approach has been validated in a case study on reuse from railway to avionics. In collaboration with practitioners, we were able to apply the approach to reuse assurance information compliant with EN 50128 in a DO-178 project. The application resulted in the reuse of all the railway artefacts, full compliance demonstration for almost 20% of the elements of the target assurance project, and almost a 75% of compliance needs coverage. Practitioners further estimated that the use of the reuse approach could lead to effort reduction by above 50% and cost reduction by above 25%. Therefore, we argue that the approach can be effectively applied and that it can reduce the cost of safety certification across standards and domains. We further conclude that it is a promising way of making cross-domain reuse more cost-effective in industry.

As future work, semantically enriching the maps, further taking terminological aspects into account, and increased, more automated tool assistance are aspects from which the reuse approach might benefit. We are also interested in conducting a case study with some goal-based standard and a different one to gain insights into possible further needs for the reuse approach, such as those that might arise from having to provide an assurance case.

Acknowledgement. The research leading to this paper has received funding from the FP7 programme under grant agreement n° 289011 (OPENCROSS). The authors also thank the OPENCROSS partners who provided input for and feedback on the approach presented in the paper and its validation, especially Franck Aimé, Katrina Attwood, Cédric Chevrel, Tim Kelly, and Cyril Marchand.

References

1. Knight JC. Safety critical systems: challenges and directions. ICSE 2002, pp. 547–550.
2. Rushby J. Just-in-time certification. ICECCS 2007, pp. 15–24.
3. RTCA DO-178C/EUROCAE ED-12c. Software Considerations in Airborne System and Equipment Certification, 2011
4. IEC 61508. Functional safety of electrical/electronic/programmable electronic safety related systems, 2011.
5. UK Ministry of Defence. Interim Defence Standard 00-56, Issue 3: Safety Management Requirements for Defence Systems. Part 2: Guidance on Establishing a Means of Complying with Part 1, 2004.
6. CENELEC. EN 50128 - Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems, 2011.
7. ISO 26262. Road vehicles — Functional safety, 2011.
8. Boeing. Certifying Boeing's Airplanes. Online, <http://787updates.newairplane.com/Certification-Process> (accessed 24-Jan-16)
9. Gill NS. Reusability issues in component-based development. ACM SIGSOFT Software Engineering Notes, 28(4): 4–4, 2003.
10. RTCA DO-297/EUROCAE ED-124 Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations, 2005.
11. Sommerville I. Software Engineering (10th ed.). Pearson, 2015.
12. Nair S, de la Vara JL, Sabetzadeh M, Briand L. An Extended Systematic Literature Review on Provision of Evidence for Safety Certification. Information and Software Technology 56(7): 689-717, 2014
13. Nair S, de la Vara JL, Sabetzadeh M, Falessi D. Evidence Management for Compliance of Critical Systems with Safety Standards: A Survey on the State of Practice. Information and Software Technology 60: 1-15, 2015
14. de la Vara JL, Borg M, Wnuk K, Moonen L. An Industrial Survey of Safety Evidence Change Impact Analysis Practice. IEEE Transactions on Software Engineering, accepted paper, 2016
15. Martin H, Baumgart S, Leitner A, Watzenig D. Challenges for reuse in a safety-critical context: A state-of-practice study. SAE Technical Paper 2014-01-0218, 2014

16. Machrouh J, Blanquart JP, Baufreton P, Boulanger JL, Delseny H, Gassino J, Ladier G, Ledinot E, Leeman M, Astruc JM. Cross domain comparison of System Assurance. ERTS-2012, pp. 1–3.
17. Ruiz A, Larrucea X, Espinoza H, Aime F, Marchand C. An Industrial Experience in Cross Domain Assurance Projects. EuroSPI 2015, pp. 29–38.
18. Chevrel C. Avionics System Certification, Certification Together Conference, 2011.
19. FAA Advisory Circular: AC 20-148 Reusable Software Components, 2004.
20. Eveleens RLC. RTO-EN-SCI-176 Integrated Modular Avionics Development Guidance and Certification Considerations, 2006.
21. CENELEC. EN 50126 - Railway applications — The specification and demonstration of reliability, availability, maintainability and safety (RAMS), 1999.
22. CENELEC. EN 50129 - Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling, 2003.
23. CENELEC. TR 50506-2: Railway applications - Communication, signalling and processing systems - Application Guide for EN 50129, Part 2: Safety Assurance, 2009.
24. Laprie JC. Dependability: Basic Concepts and Terminology. Springer, 1992.
25. Li J, Zhang HC, Lin Z. Asymmetric negotiation based collaborative product design for component reuse in disparate products. *Comput. Ind. Eng.* 57(1): 80–90, 2009.
26. Krohn CA. Space Shuttle Component Reuse Study. *IEEE Trans. Reliab.* R-25(4): pp. 234–238, 1976.
27. Jha M, O'Brien L. A comparison of software reuse in software development communities. MySEC 2011, pp. 313–318.
28. Salinesi C, Mazo R, Djebbi O, Diaz D, Lora-Michiels A. Constraints: The core of product line engineering. RCIS 2011, pp. 1–10.
29. Harn H, Berzins V, Luqi. Software evolution via reusable architecture. ECBS 1999, pp. 11–17.
30. Obbink H, Pohl K (Eds.). *Software Product Lines*. Springer, 2005.
31. van der Linden F (Ed.). *Software Architectures for Product Families*. Springer, 2000.
32. Mangun D, Thurston DL. Incorporating component reuse, remanufacture, and recycle into product portfolio design. *IEEE Trans. Eng. Manag.* 49(4): 479–490, 2002.
33. Amelia L, Wahab DA, Che Haron CH, Muhamad N, Azhari CH. Initiating automotive component reuse in Malaysia. *J. Clean. Prod.* 17(17): 1572–1579, 2009.
34. Go TF, Wahab DA, Rahman MNA, Ramli R, Hussain A. Genetically optimised disassembly sequence for automotive component reuse. *Expert Syst. Appl.* 39(5): 5409–5417, 2012.
35. Zeller M, Höfig K, Rothfelder M. Towards a Cross-Domain Software Safety Assurance Process for Embedded Systems. SASSUR 2014, pp. 396–400.
36. Papadopoulos Y, McDermid JA. The potential for a generic approach to certification of safety critical systems in the transportation sector. *Reliab. Eng. Syst. Saf.* 63(1):47-66, 1999.
37. pSAFECER project. Deliverable “Definition of cross-domain use case description, use case-specific requirements and assessment criteria”, 2012.
38. Gallina B, Kashiyaandi S, Zugsbratl K, Geven A. Enabling Cross-Domain Reuse of Tool Qualification Certification Artefacts. SAFECOMP Workshops 2014, pp. 255-266
39. Gallina B, Szatmári Z. Ontology-Based Identification of Commonalities and Variabilities Among Safety Processes. PROFES 2015, pp. 182-189
40. Gallina B. A Model-Driven Safety Certification Method for Process Compliance. ISSREW 2014, pp. 204–209.
41. Rodriguez-Dapena P. Software safety certification: a multidomain problem. *IEEE Softw.* 16(4): 31–38, 1999.
42. Zeng F, Lu M, Zhong D. Software Safety Certification Framework Based on Safety Case. CSSS 2012, pp. 566–569.
43. OPENCROSS project. OPENCROSS Platform - Final Prototype User Manual. Online, <http://www.opencross-project.eu/node/7>, 2014 (accessed 24-Jan-16)
44. OPENCROSS project. Deliverable D4.4 - Common Certification Language: Conceptual Model, version 1.4. Online, <http://www.opencross-project.eu/node/7>, 2015 (accessed 24-Jan-16)
45. de la Vara JL, Ruiz A, Attwood K, Espinoza H, Panesar-Walawege RK, Lopez A, del Rio I, Kelly T. Model-Based Specification of Safety Compliance Needs: A Holistic Generic Metamodel. *Information and Software Technology* 72: 16-30, 2016.
46. OPENCROSS project. Deliverable D5.2 - Detailed requirements for the OPENCROSS compositional certification approach. Online, <http://www.opencross-project.eu/node/7>, 2012 (accessed 24-Jan-16)
47. OPENCROSS project. Deliverable D1.2 - Use cases description and business impact. Online, <http://www.opencross-project.eu/node/7>, 2012 (accessed 24-Jan-16)
48. OPENCROSS project. Deliverable D1.4 - Implementation of use cases on top of OPENCROSS platform. Online, <http://www.opencross-project.eu/node/7>, 2015 (accessed 24-Jan-16)

49. OPENCROSS project. Deliverable D1.3 - Evaluation framework and quality metrics, version 1.2. Online, <http://www.opencross-project.eu/node/7>, 2013 (accessed 24-Jan-16)
50. OPENCROSS project. Deliverable D1.5 - OPENCROSS Benchmarking. Online, <http://www.opencross-project.eu/node/7>, 2015 (accessed 24-Jan-16)
51. Esposito, D. Cotroneo, N. Silva, "Investigation on Safety-related Standards for Critical Systems", 2011 First International Workshop on Software Certification
52. Terry Costlow "Security guideline set to provide structure for connected vehicles", 16-Dec-2015 01:57 EST Web:<http://articles.sae.org/14503/>
53. NHTSA, "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application", U.S Department of Transportation, August 2014
54. NHTSA, "Assessment of the Information Sharing and Analysis Center Model U.S Department of Transportation, October 2014
55. NHTSA, "A Summary of Cybersecurity Best Practices", U.S Department of Transportation, October 2014
56. NHTSA, "Characterization of Potential Security Threats in Modern Automobiles", U.S Department of Transportation, October 2014
57. NHTSA, "National Institute of Standards And Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles", U.S Department of Transportation, October 2014